

We claim:

1. A method providing security for a plurality of data records stored on a computer-readable medium within a computing system, wherein

said computer readable medium additionally stores a first data structure, starting at a first location within said computer readable medium, locating data records in said plurality thereof,

said method comprises an encryption subroutine executed as said computing system is being shut down and a decryption subroutine executed as said computing system is being initialized,

said encryption subroutine includes receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure to produce an encrypted version of said first data structure, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location.

2. The method of claim 1, wherein said second location is on said computer readable medium

3. The method of claim 2, wherein said second location is at said first location.

4. The method of claim 1, wherein said nonvolatile storage is a memory structure, separate from said computer readable medium, within said computing system.

5. The method of claim 1, wherein
 encryption of said first data structure occurs within a cryptographic processor
 in said computing system using an encryption key,
 said cryptographic processor is separate from a system processor within said
 computing system, and
 decryption of said encrypted version of said first data structure occurs within
 said cryptographic processor in said computing system using a decryption key
 generated from data stored in secure storage accessed by said cryptographic
 processor.

6. The method of claim 1, wherein
 a public key of said computing system is used for encryption of said first data
 structure, and
 a private key of said computing system is used for decryption of said
 encrypted version of said first data structure.

7. The method of claim 1, wherein said encrypted version of said first data
 structure is equal in length to said first data structure.

8. The method of claim 1, wherein
 said computer readable medium additionally stores a second data structure,
 starting at a second location within said computer readable medium, describing
 characteristics of said first data structure, and
 said encryption subroutine additionally includes reading said second data
 structure to determine characteristics of said first data structure.

9. The method of claim 8, wherein
 said first data structure is a file allocation table, and

3 said second data structure is a boot record.

1 10. The method of claim 8, wherein
2 said first data structure includes an array of file records in a master file table
3 of a NTFS file, and
4 said second data structure includes metafile data in said master file table.

1 11. The method of claim 1, wherein
2 said method additionally comprises a configuration subroutine providing a
3 user interface for setting and resetting a configuration bit, and
4 said encryption subroutine is executed according to a state of said
5 configuration bit.

1 12. The method of claim 11, wherein
2 said encryption subroutine additionally includes setting a flag bit in non-
3 volatile storage, and
4 said decryption subroutine is executed only when said flag bit is set.

1 13. A method providing security for a plurality of data records stored on a
2 computer readable medium within a computing system, wherein
3 said computer medium additionally stores a first data structure starting at a
4 first location within said removable computer readable medium, locating data
5 records in said plurality thereof,
6 said method comprises an encryption subroutine executed to encrypt said
7 first data structure and a decryption subroutine subsequently executed to decrypt
8 an encrypted version of said first data structure,
9 said encryption subroutine includes reading said first data structure from said
10 computer readable medium, encrypting said first data structure within a
11 cryptographic processor in said computing system using an encryption key to

12 produce an encrypted version of said first data structure, deleting said first data
 13 structure from said computer readable medium, and storing said encrypted version
 14 of said first data structure in nonvolatile storage, starting at a second location within
 15 said nonvolatile storage, and

16 said decryption subroutine includes reading said encrypted version of said
 17 first data structure from said nonvolatile storage, decrypting said encrypted version
 18 of said first data structure within said cryptographic processor in said computing
 19 system using a decryption key generated from data stored in secure storage
 20 accessed by said cryptographic processor to form said first data structure, and
 21 writing said data structure to said computer readable medium, starting at said first
 22 location.

1 14. The method of claim 13, wherein
 2 said encryption subroutine is executed in response to receiving a request to
 3 shut down said computing system, and
 4 said decryption subroutine is executed in response to electrical power being
 5 turned on within said computing system.

1 15. The method of claim 14, wherein
 2 said method additionally comprises a configuration subroutine providing a
 3 user interface for setting and resetting a configuration bit, and
 4 said encryption subroutine is executed according to a state of said
 5 configuration bit.

1 16. The method of claim 15, wherein
 2 said encryption subroutine additionally includes setting a flag bit in non-
 3 volatile storage, and
 4 said decryption subroutine is executed only when said flag bit is set.

1 17. The method of claim 13, wherein

2 said method additionally comprises a cryptographic selection subroutine
3 providing a graphical user interface,

4 said cryptographic selection subroutine includes displaying a choice between
5 encryption and decryption, displaying representations of computer readable medium
6 in said computing system, and receiving a cryptographic selection signal indicative
7 of whether encryption or decryption is to occur and of a chosen computer readable
8 medium,

9 said encryption subroutine is executed in response to receiving a
10 cryptographic selection signal indicating encryption is to occur, with said first data
11 structure of said chosen computer readable medium being encrypted, and

12 said decryption subroutine is executed in response to receiving a
13 cryptographic selection signal indicating decryption is to occur, and with said
14 encrypted version of said first data structure of said chosen computer readable
15 medium being decrypted.

1 18. The method of claim 17, wherein said encrypted version of said first data
2 structure is stored in nonvolatile storage on said chosen computer readable
3 medium.

1 19. A computing system providing secure storage of a plurality of data records
2 comprising:

3 a first computer readable medium storing said plurality of data records and
4 a first data structure providing locations and sequences for accessing data within
5 said data records;

6 a first drive unit recording data on said first computer readable medium and
7 reading data from said computer readable medium;

8 nonvolatile storage;

9 a cryptographic processor, wherein said cryptographic processor is

10 programmed to execute an internal encryption routine to encrypt a data structure,
 11 forming an encrypted version of said data structure using an encryption key, and to
 12 execute subsequently an internal decryption routine, decrypting said encrypted
 13 version of said data structure, using a decryption key;

14 secure storage, accessed by said cryptographic processor, holding data used
 15 within said cryptographic processor to derive said decryption key;

16 a microprocessor, separate from said cryptographic processor, wherein said
 17 microprocessor is programmed to execute a data structure encryption routine to
 18 encrypt said first data structure and to execute subsequently a data structure
 19 decryption routine to decrypt an encrypted version of said first data structure,
 20 wherein said data structure encryption routine includes causing said cryptographic
 21 processor to read said first data structure from said computer readable medium, to
 22 execute said internal encryption routine, encrypting said data structure to form said
 23 encrypted version of said first data structure, and to write said encrypted version of
 24 said first data structure to nonvolatile storage, wherein said first data structure is
 25 additionally deleted from said first computer readable medium during execution of
 26 said data structure encryption subroutine, and wherein said data structure
 27 decryption subroutine includes causing said cryptographic processor to read said
 28 encrypted version of said first data structure from nonvolatile storage, to decrypt
 29 said encrypted version of said first data structure, forming said first data structure,
 30 and to write said first data structure to said computer readable medium, starting at
 31 said first location.

- 1 20. The computing system of claim 19, wherein
- 2 said first drive unit is a hard drive,
- 3 said data structure encryption subroutine is executed in response to receiving
- 4 a request to shut down said computing system, and
- 5 said data structure decryption subroutine is executed in response to electrical
- 6 power being turned on within said computing system.

21. The computing system of claim 20, wherein
said microprocessor is additionally programmed to execute a configuration
subroutine providing a user interface for setting and resetting a configuration bit,
and
said encryption subroutine is executed according to a state of said
configuration bit.

22. The computing system of claim 21, wherein
said encryption subroutine additionally includes setting a flag bit in non-
volatile storage, and
said decryption subroutine is executed only when said flag bit is set.

23. The computing system of claim 19, wherein
said computer readable medium is removable,
said method additionally comprises a cryptographic selection subroutine
providing a graphical user interface,
said cryptographic selection subroutine includes displaying a choice between
encryption and decryption, displaying representations of computer readable medium
in said computing system, and receiving a cryptographic selection signal indicative
of whether encryption or decryption is to occur and of a chosen computer readable
medium,
said encryption subroutine is executed in response to receiving a
cryptographic selection signal indicating encryption is to occur, with said first data
structure of said chosen computer readable medium being encrypted, and
said decryption subroutine is executed in response to receiving a
cryptographic selection signal indicating decryption is to occur, and with said
encrypted version of said first data structure of said chosen computer readable
medium being decrypted.

24. The computing system of claim 23, wherein said encrypted version of said

2 first data structure is stored in nonvolatile storage on said chosen computer
3 readable medium.

1 25. The computing system of claim 19, wherein
2 said computer readable medium additionally stores a second data structure,
3 starting at a second location within said computer readable medium, describing
4 characteristics of said first data structure, and
5 said data structure encryption subroutine additionally includes reading said
6 second data structure to determine characteristics of said first data structure.